

WHAT IS CLAIMED

1       1. A method for authenticating a first party at a  
2 second party, comprising:

3           (a) receiving a random number from said first party  
4 as a first challenge;

5           (b) incrementing a count value in response to  
6 receiving said first challenge;

7           (c) generating a first challenge response by  
8 performing a keyed cryptographic function (KCF) on said  
9 first challenge and said count value using a first key;

10          (d) transferring said count value, as a second  
11 challenge, and said first challenge response to said  
12 first party;

13          (e) receiving a second challenge response from said  
14 first party, said second challenge response being a  
15 result of performing said KCF on said second challenge  
16 using said first key; and

17          (f) verifying said first party based on said second  
18 challenge and said second challenge response.

1       2. The method of claim 1, prior to said step (c),  
2 further comprising:

3           (g) generating said first key using a root key.

1       3. The method of claim 1, wherein said step (c)  
2 generates said first challenge response by performing  
3 said KCF on said first challenge, said count value, and  
4 an identifier for said second party using said first key.

1       4. The method of claim 1, further comprising:

2                 (g) establishing a second key based on said first  
3 and second challenges.

1                 5. The method of claim 1, wherein said step (a)  
2 receives a global challenge as | said first challenge from  
3 said first party.

1                 6. The method of claim 1, wherein said first party  
2 is a network of a wireless system and said second party  
3 is a mobile.

1                 7. The method of claim 6, wherein said step (c)  
2 generates said first challenge response by performing  
3 said KCF on said first challenge, said count value and  
4 type data using said first key, said type data indicating  
5 a type of protocol being performed by said network and  
6 said mobile.

1                 8. The method of claim 6, wherein said step (c)  
2 generates said first challenge response by performing  
3 said KCF on said first challenge, said count value, an  
4 identifier for said mobile, and type data using said  
5 first key, said type data indicating a type of protocol  
6 being performed by said network and said mobile.

1                 9. The method of claim 6, further comprising:  
2                 (g) establishing a second key based on said first  
3 and second challenges.

1                 10. The method of claim 9, wherein said second key  
2 is one of secret shared data and a session key.

2025-2925-161P

1       11. The method of claim 6, wherein said step (b)  
2 increments said count value using a bit counter of  
3 greater than 64 bits and which was initialized using a  
4 random number.

1       12. A method for authenticating a first party at a  
2 second party, comprising:

3           (a) outputting a random number as a first challenge;  
4           (b) receiving a second challenge and a first  
5 challenge response from said first party, said second  
6 challenge being a count value, and said first challenge  
7 response being a result of performing a keyed  
8 cryptographic function (KCF) on said first challenge and  
9 said count value using a first key; and  
10          (e) verifying said first party based on said first  
11 challenge, said second challenge, and said first  
12 challenge response.

1       13. The method of claim 12, further comprising:

2           (f) establishing a second key based on said first  
3 and second challenges.

1       14. The method of claim 12, wherein said step (a)  
2 outputs said first challenge as a global challenge.

1       15. The method of claim 12, wherein said first party  
2 is a mobile of a wireless system and said second party is  
3 a network.

1       16. The method of claim 15, further comprising:

25TE20-2925-161P

2                 (f) establishing a second key based on said first  
3 and second challenges.

1                 17. The method of claim 16, wherein said second key  
2 is one of secret shared data and a session key.

1                 18. The method of claim 12, further comprising:  
2                 (f) generating a second challenge response by  
3 performing said KCF on said second challenge using said  
4 first key; and

5                 (g) transferring said second challenge response to  
6 said second party.

1                 19. The method of claim 18, wherein said step (f)  
2 generates said second challenge response by performing  
3 said KCF on said second challenge and an identifier for  
4 said second party using said first key.

1                 20. The method of claim 18, wherein said first party  
2 is a mobile of a wireless system and said second party is  
3 a network.

1                 21. The method of claim 20, wherein said step (f)  
2 generates said second challenge response by performing  
3 said KCF on said second challenge and type data using  
4 said first key, said type data indicating a type of  
5 protocol being performed by said network and said mobile.

202522760

1           22. The method of claim 20, wherein said step (f)  
2 generates said second challenge response by performing  
3 said KCF on said second challenge, an identifier for said  
4 network, and type data using said first key, said type  
5 data indicating a type of protocol being performed by  
6 said           network           and           said           mobile.